Homeland Security

DHS S&T Silicon Valley Innovation Program (SVIP)

SOFTWARE SUPPLY CHAIN VISIBILITY TOOLS

Other Transaction Solicitation Call # 70RSAT22R00000027

https://www.dhs.gov/science-and-technology/svip
DHS-Silicon-Valley@hq.dhs.gov

1. Introduction

This Other Transaction Solicitation (OTS) Call 70RSAT22R00000027 is being issued against the Department of Homeland Security (DHS), Science & Technology (S&T), Silicon Valley Innovation Program (SVIP)[1], 5-Year Innovation OTS (70RSAT21R00000006). All terms and conditions of the DHS S&T SVIP 5-Year Innovation OTS (70RSAT21R00000006) remain incorporated into this Call unless otherwise noted herein.

The U.S. DHS is committed to using cutting-edge technologies and scientific talent in its quest to make America safer. SVIP, on behalf of DHS Operational Components, invests in startup companies with viable technologies suitable for rapid prototyping projects from across the nation and around the world to adapt, develop, and harness cutting-edge capabilities that are commercially sustainable while simultaneously meeting the needs of DHS Operational Components and Programs.

1.1 DHS Operational Need

Software has become a key component of infrastructure systems that individuals and organizations rely upon for essential services, including communications, finance, transportation, and energy. Attacks that exploit vulnerabilities in software can lead to outages or damage to safety- and life-critical systems. Strengthening the assurance of the software supply chain is essential to protecting software and software-controlled systems. Transparency is a necessary foundation for a high-assurance supply chain, enabling answers to questions like: What software components are in the system? Who built those components? What other software do those components depend upon?

A Software Bill of Materials (SBOM) "is a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships."[2] Tools that support wide availability of trustworthy SBOMs can enable stakeholder visibility into software supply chains and new risk assessment capabilities.

We intend to energize the market to provide SBOM-based capabilities for stakeholders within the enterprise, system administrator and software developer communities. We seek both foundational open-source software libraries and value-added tooling.

This SVIP Call seeks technical capabilities that could serve the mission needs of one or more DHS Operational Components and Programs including:

- Cybersecurity and Infrastructure Security Agency (CISA)

1.2 Illustrative Scenarios

The following illustrative scenarios are intended to describe where the technologies being sought by DHS in this topic call could potentially be applied. **DHS is not necessarily seeking the technologies for these specific scenarios but instead are providing them to give some context for interested parties.**

[1] https://www.dhs.gov/science-and-technology/svip
[2] https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf

However, given that responses to this OTS Call may be relevant to these and other scenarios, it is expected that an applicant will use one or more of these stakeholder scenarios to frame their application.

1.2.1 Scenario I: Enterprise Perspective

Nick Rubenstein's boss called again, so he jumped off his call, and answered. Skipping past their usual greetings, Sara Kim dove right in "This request comes straight from the board of our whole hospital chain. We need to know what our exposure is to this new vulnerability, Log4Dale. How soon can we give them an answer? And how soon until you can tell me what kind of answer we'll give them?" An IT risk analyst, Nick and his small team had prepped for this, but the process hadn't been tested.

He pulled up the dashboard for his asset management system as a starting point. This, in theory, should tell them all the software that was on their organization's network. But they were still discovering assets that weren't yet being recorded. They used outside scanners, and checked them against the asset inventory, but this had been hampered by some confusion of which systems were called what; particularly when different security vendors used different names, it sometimes required manual disambiguation.

Once he felt that list was complete, Nick turned his attention to the dependency data: what was actually running inside all those blinking boxes and advanced applications on the network. They had done the groundwork to map the asset data to SBOM data. Now, the visualization application that he and his team had built searched through the SBOM data to determine which software might be affected and which—more importantly—could be easily ignored for this risk calculation. He reached out to the security operations center (SOC) to get access to the list of Vulnerability Exploitability eXchange (VEX) documents, which provided assertions from the software suppliers that their products were not actually affected. These were correlated and displayed for analysis as part of a comprehensive visualization, and the list of risks to Nick's company shrank further.

Now came the hard part: determining the actual exposure for the remaining risk. Sara had already pulled the rest of the team together, each pulling data from different tools to understand which of the assets with risky dependencies were exposed, and where controls were already in place. The threat team was able to confirm that while exploitation was likely, there was not yet evidence of automated scans by bad actors to exploit this risk. Because of the groundwork that had been done to integrate SBOM information, and the ability to visualize the complex software enterprise, Nick and Sara had time to pull together their complete analysis to provide a response to their board.

1.2.2 Scenario II: System Administrator Perspective

Ajay's collaboration application issued another ping, as another task was added to the SOC's list of "things to manage." He pulled up his Security Incident and Event Management (SIEM) dashboard and loaded a set of new tools. The security team was worried about a new imaging system that the hospital was installing, not least because it had a massive integrated data functionality that required it to talk to a bunch of other data systems—his systems. What was even in this thing? He pulled up the SBOM data

and winced as the cursor spun while it tried to build a graph visualization of the ten thousand-odd dependencies that just the network interface application used. At that point, he dumped the SBOM into a plug-in for the SIEM and made sure that it automatically updated for software updates. The system was already analyzing the SBOM data for known vulnerabilities. Another wince, as the list grew before him on the screen. Like many SOC analysts, he knew that most warnings could be ignored, but the ones that couldn't would get you if you make mistakes.

Fortunately, a suite of new tools for the SOC was part of their approach to automate much of the manual processes employed by their security team. A few keystrokes allowed him to do some basic triage: which vulnerabilities were on CISA's Known Exploited Vulnerability (KEV) list? Some affected components already had solutions being pushed by the open-source maintainers: those were tagged to monitor to see how long it took the medical device manufacturer to update. A report about this timing would be sent up to the Chief Information Security Officer (CISO) and the procurement team. Another alert flagged that the SBOM for the third-party application that linked to the imaging system was for an earlier version than what had been installed the previous evening. There must be a flaw with the Digital Bill of Materials (DBOM) server—he created a new ticket to determine whether it was on the hospital or the vendor's end, and tagged it to his colleague, Katie. Ajay was thankful that automation tools integrated with the SIEM software allowed him to complete his tasks in a timely and efficient manner to keep his network secure and operational.

1.2.3 Scenario III: Software Developer Perspective

Brenda O'Malley arrives at Software Supreme, Inc (SSI) to begin her daily work as a senior software developer. Brenda is part of a team creating a new version of SSI's flagship product, MyAgent. The new version will require the addition of code implementing Generative Adversarial Networks (GANs). While Brenda could implement a GAN capability herself, she knows that if she can leverage an existing high-quality GAN implementation, she could spend her time adding unique value to the MyAgent software.

Brenda launches her Interactive Development Environment (IDE) and searches for GAN software libraries that are compatible with her language and runtime environment. Using relevant plug-ins, the IDE identifies a few candidate libraries. Brenda uses the IDE's new SBOM functions to review the provenance of the candidate libraries; software dependencies; and known vulnerabilities, along with their severities and mitigations. Some of the candidate libraries have extensive dependencies on codebases of variable quality (i.e., some with many unpatched vulnerabilities). The beGAN library and the GAiN library are maintained by development teams that Brenda knows and respects, vulnerabilities are patched promptly, and the code has no outstanding vulnerabilities without reasonable mitigations. To choose between these two libraries, Brenda looks at the mitigations highlighted by the IDE and concludes that the beGAN library is a somewhat better fit for MyAgent.

Brenda discusses the options with her team, and they commit to using the beGAN library. Using her IDE, she installs beGAN, reviews the interfaces to its functions, and adjusts the software design for the new MyAgent. In the following weeks, Brenda and her team write the new code for MyAgent, regularly committing their changes into SSI's Continuous Integration (CI) system. The CI system's build automation component uses its new SBOM functionality to automatically generate SBOM artifacts for each new build of the MyAgent software. When the new version of MyAgent ships to customers, the

SBOM record is included. SSI also makes the MyAgent SBOM available to prospective customers to support their product selection decisions.

2. Topic Description

To fully realize the benefits of SBOMs and software component transparency, machine processing and automation are necessary. This requires widespread interoperability across the supply chain which, in turn, requires standardized data formats and identification schemes. Unfortunately, diverse needs within the software ecosystem have resulted in multiple candidate SBOM data formats and identification schemes that stakeholder tools must handle correctly. Utility software that translates among many of the more common formats and identification schemes will be essential to enable a flexible SBOM tooling ecosystem. While stand-alone tools exist for generating SBOMs in each of the common formats, the need to automatically generate an SBOM during the software build process requires SBOM generators designed to integrate into (i.e., plug in) to build systems.

As shown in the illustrative scenarios, additional tools will be needed to enable human use of machine-readable SBOM data objects that encode software identity and provenance. For business-focused (rather than technology-focused) analysts, tools that support visualization of software provenance and risk, potentially in the context of a specific regulatory domain (e.g., health care, finance) can support risk-informed decisions. Software developers will require capabilities that plug in to popular IDE tools, highlighting software dependencies, warning of vulnerabilities, and providing information about critical mitigations. System administrators use Security Incident and Event Management (SIEM) tools to consolidate security threat information and understand which threats may apply to systems deployed within the operational environment. Capabilities that leverage software identifiers (encoded in SBOMs and vulnerability records) can help SIEM tools to pinpoint vulnerable operational systems and enable system administrators to prioritize mitigations.

2.1 Core SBOM Fields

Field	SPDX	SWID	CycloneDX
Supplier	(3.5) PackageSupplier:	<Entity> @role (softwareCreator/ publisher), @name	publisher
Component	(3.1) PackageName:	<softwareIdentity> @name	name
Unique Identifier	(3.2) SPDXID:	<softwareIdentity> @tagID	bom/serialNumber and component/bom-ref
Version	(3.3) PackageVersion:	<softwareIdentity> @version	version
Component Hash	(3.10) PackageChecksum:	<Payload>/../<File> @[hash-algorithm]:hash	hash
Relationship	(7.1) Relationship: CONTAINS	<Link>@rel, @href	(Nested assembly/subassembly and/or dependency graphs)
SBOM Author	(2.8) Creator:	<Entity> @role (tagCreator), @name	bom-descriptor: metadata/manufacture/ contact

2.2 Topic Call Conventions

The International Organization for Standardization (ISO) uses specific verbal forms to convey clarity based on type of statement. This Topic Call adopts and uses the following ISO document conventions:

- Requirements - SHALL, SHALL NOT
- Recommendations - SHOULD, SHOULD NOT
- Permission - MAY, MAY NOT
- Possibility and Capability - CAN, CANNOT

3. Technical Topic Areas (TTAs)

DHS seeks technologies and solutions that address this need via the following TTAs.

Responses from offerors SHALL be any combination of the TTAs that includes TTA #1.

3.1 TTA #1 [REQUIRED]: Foundational Open-Source Libraries

To ensure broad adoption and deployment of the capabilities that are sought in this Call, DHS requires that two core capabilities be delivered as open-source software libraries with the following properties:

- Fully documented source code
- Test suites/artifacts to test and verify the libraries
- Provided under an open-source license that ensures that the software is patent free, royalty free, non-discriminatory, available to all and free to implement on a global basis. e.g., Apache License

2.0[3], MIT License[4] etc.

1. Multi-format SBOM Translator

   This library must be capable of reading, translating between, and writing at a minimum, the core SBOM fields (See Section 2.1) of the following common SBOM data formats which are Software Package Data Exchange (SPDX), Software Identification (SWID) Tags, and CycloneDX. Translation among additional SBOM data formats is welcome.

2. Software Component Identifier Translator

   This library must be capable of mapping identifiers of software components across the following identification systems. At a minimum, they should be able to map across Common Platform Enumeration (CPE), SWID Tags, Package URLs (purls), and SoftWare Heritage persistent Identifiers (SWHIDs). Translation among additional software component identification systems is welcome.

Given the foundational nature of this TTA, and to reduce duplication of effort, companies awarded under this Call must work together as a cohort, in a public and transparent manner. The ability to accept and incorporate public technical community input and feedback is required to ensure that these open-source libraries will be broadly useful to the global technical community.

3.2 TTA #2: Automated SBOM Generation

DHS seeks a capability that can be integrated into the Software Development Lifecyle (SDLC) that can automate the creation and updating of SBOMs. Potential points of integration include (a non-exhaustive list):

- As part of a continuous integration pipeline
- As part of source control management infrastructure
- As part of a standalone build cycle

Implementations of this capability SHALL incorporate the open-source libraries that are described in TTA #1

3.3 TTA #3: SBOM Enabled Vulnerability Visualization

DHS seeks a visualization capability that can access and read SBOMs that may be in a variety of data formats, link that information with external records of vulnerabilities and severity information from trusted sources, and provide information on available patches and mitigations.

Implementations of this capability SHALL incorporate the open-source libraries that are described in TTA #1

[3] https://choosealicense.com/licenses/apache-2.0/
[4] https://choosealicense.com/licenses/mit/

3.4 TTA #4: SBOM Enabled IDE Plug-in

DHS seeks to develop SBOM enabled IDE Plug-ins that will provide a software developer the ability to read and visualize:

- SBOM information
- Links to Common Vulnerabilities and Exposures (CVEs) or other records of vulnerabilities associated with the function, library, and related code,
- Information identifying severity, (e.g., Common Vulnerability Scoring System (CVSS) score, Stakeholder-Specific Vulnerability Categorization (SSVC)), susceptibility conditions
- Information about available patches and mitigations

The add-in SHOULD support the open-source versions of the two most popular IDEs by market share, and MAY support other popular IDEs.

Implementations of this capability SHALL incorporate the open-source libraries that are described in TTA #1

3.5 TTA #5: SBOM Enabled SIEM Plug-In

DHS seeks to develop SBOM enabled Plug-ins that can be integrated with existing SIEM tools that analyze security events from various sources, display patterns of activity in the context of the computing (e.g., enterprise) environment, and generate alerts for immediate attention.

Within the usual SIEM dashboards, a Plug-in will display information about vulnerabilities that are known to affect currently operational software, including:

- Indication of which enterprise platforms (e.g., physical hosts, virtual machines, containers) are running the affected software, affected system services and applications
- Links to CVEs (or other records of vulnerabilities) associated with the software
- Severity information (e.g., CVSS score, SSVC), susceptibility conditions
- Information about available patches and mitigations

The extension SHOULD support the two most popular SIEM products by market share, and MAY support other popular SIEM products.

Implementations of this capability SHALL incorporate the open-source libraries that are described in TTA #1

4. Project Deliverables and Phases

The SVIP is generally structured in 4 Phases, with an opportunity to award a Phase 5 for further testing/piloting in additional operational environments and potentially addressing additional use cases. For the purposes of this project, all applicants shall submit a Phase 1 application.

SVIP Phase detail is listed in the following chart:

Phase	Funding Level & Source	Deliverables	Due Date
1	$50,000 to $200,000	Minimum Viable Product demonstrating proof-of-concept of adaptation	3–9 months after award
2	$50,000 to $500,000	Prototype development building out all features to demonstrate viability	3–9 months after successful completion of Phase 1
3	$50,000 to $500,000	Prototype deployed in realistic T&E environment for independent T&E and red teaming	3–9 months after successful completion of Phase 2
4	$50,000 to $500,000	Operational testing of developed capability fully coordinated with DHS component and operational stakeholders	3-9 months after successful completion of Phase 3
5	TBD at the Government's discretion	Additional operational testing which may include additional use cases in additional operational environments	Begin after successful completion of Phase 4

Referring to the table above, the required milestones and deliverables for each phase shall incorporate the objectives defined as follows:

- **Phase 1:** Delivery of a Minimum Viable Product that demonstrates proof-of-concept and supporting documentation inclusive of verifiable test evidence, technical drawings, and software demonstrations or other proof that the technical approach to address a DHS requirement or challenge as identified in this Call is sound. At the end of this Phase, successful applicants will have:
    - Created a proof of concept of a new technology suitable for demonstration, or
    - Produced reviewable modifications to pre-existing technologies suitable for demonstration, or
    - Documented a go-to-market commercialization strategy
    - Cohort collaboration and community contribution report regarding the development of the TTA #1 Foundational Open-Source Libraries
- **Phase 2**: An end-to-end working prototype with full capabilities. Objectives of this phase are to use the results of Phase 1 to build out all features and functions in the prototype to demonstrate viability. At the end of Phase 2, the prototype must:
    - Demonstrate end-to-end operational viability
    - Be ready for independent review and evaluation
    - Validate the commercialization strategy with potential customers and partners
    - Cohort collaboration and community contribution report regarding the development of the TTA #1 Foundational Open-Source Libraries
- **Phase 3**: A production ready prototype that will be deployed into a realistic test and evaluation environment to experiment against realistic conditions and undergo an independent test and evaluation process to ensure operational suitability. These tests will be fully coordinated with the DHS component and operational stakeholders and it is anticipated that all independent testing

feedback will be incorporated into the technology solution by the end of this Phase. Objectives of this phase are to:
    - Demonstrate a fully functional end to end capability
    - Support the functional, security, privacy, and interoperability testing and validation of the capability by an independent Red Team
    - Incorporate the feedback and results of the independent test into the prototype
    - Cohort collaboration and community contribution report regarding the development of the TTA #1 Foundational Open-Source Libraries
- **Phase 4**: Delivery of technologies with fully completed designs and which reputably provide all proposed features and functionality. Any tests and demonstrations in this Phase will be fully coordinated with the DHS component and operational stakeholders and may result in a limited number of prototypes or licenses of the technology to conduct the testing in multiple user scenarios and conditions. Objectives of this phase are to:
    - Deploy the capability for operational testing and demonstration
    - Incorporate and adjust the capability based on the operational testing
    - Cohort collaboration and community contribution report regarding the development of the TTA #1 Foundational Open-Source Libraries
- **Phase 5**: Phase 5 awards are made only to meet a Government need and additional testing requirements. The additional testing may be done in different environments using additional use cases. This Phase may result in a limited number of prototypes or licenses of the technology in order to test the prototype in multiple user scenarios and conditions. In order to meet an identified Government need, this phase may be funded beyond the total Phase 1-4 limits.

The Government may choose to combine and/or skip later phases which will be determined after the successful completion of the Phase 1 effort and subject to the Government's invitation. See 5-Year Innovation OTS (70RSAT21R00000006) Section 2.2.3.

For the purposes of this project, DHS S&T anticipates making Phase 1 awards of $50,000 to $200,000 in funding for each award, with an estimated period of performance of 3 to 9 months. Successful projects will be eligible for subsequent phases of funding with a ceiling range between $50,000-$500,000 per phase (or in total $200,000-$1,700,000 for Phases 1-4) and duration to be approximately six (6) to nine (9) months per phase. The ceilings of the subsequent phases are based on multiple factors such as DHS needs and available funds, DHS will provide the specific phase 2-4 ceiling amounts for this topic during the phase 2- 4 invitation process. See 5-Year Innovation OTS (70RSAT21R00000006) Section 2.2.1.

A Phase 5 may be awarded if the Government determines that further operational testing is required, and/or the technology is applicable in additional DHS use cases. Phase 5 OTAs will be scaled to fit the mission need/requirement in both cost and length of time and are not restricted by the Phases 1-4 ceilings listed above.

Project Phase awards are dependent on progress made by the applicant, DHS needs, and availability of funds. In order to receive consideration for subsequent Phases, applicants shall be invited by the Government to submit an application for each Phase. The Government reserves the right to not make subsequent Phase awards.

Phase 1 shall not exceed $200,000, and Phases 2-4 shall not exceed $500,000 per Phase for a total

of $1,700,000.

At the end of Phase 4, DHS S&T intends that successful projects shall have reached a sufficient stage of development to be production-ready for deployment, or commercial availability to stakeholders, including potential follow-on production contract or transaction by DHS.

The specific phased approach set out above is general program guidance and not a mandatory structure. At the sole discretion of the Government, each OT project award may begin at any Phase, or make use of combined or skipped Phases, in order to accommodate different technology and different maturity levels of an awardee's products. Any variations such as combining phases and/or skipping phases may be made based on technical maturity of the solutions received.

5. General Information and Instructions

5.1 Response Dates

Event	Time Due	Date or Date Due
Virtual Industry Day Register to attend at: https://sri-csl.regfox.com/svip-SSCVT-industry-day	N/A	July 14, 2022 9:30 AM – 11:30 AM PT / 12:30 PM – 2:30 PM ET*
Applications Due Date: Applications will be accepted on a continuous, rolling basis until the application deadline. The deadline for submitting an application is listed on the right. **Applications shall be received prior to the deadline to be evaluated in the review cycle.**	12:00 PM (Noon) PT / 3:00 PM ET*	October 3, 2022
Notification of Application Pre-Oral Pitch Evaluation Results	N/A	Approximately 45 days following the application deadline
Oral Pitches	N/A	Approximately 60 days following the application deadline (if requested)
Closing Date/Final Deadline	12:00 PM (noon) PT / 3:00 PM ET*	October 3, 2022

* Eastern Time (ET), Pacific Time (PT)

We encourage you to submit your application well before the deadline.

Applications and application resubmissions shall be submitted by the due dates listed above to be reviewed in that cycle. DHS will conduct reviews following each submission deadline and anticipates that reviews will be completed within approximately 45 days following each submission deadline.

Under no circumstances will applications and application resubmissions received after the Final Deadline date and time be considered for review.

DHS may decide to close the call early. If this occurs, DHS will publish a notification on SAM.gov 30 days prior to closing the call.

Applicants shall check SAM.gov for any amendments and changes to this technical Call.

5.2 Eligibility

Applicants **SHALL** determine if they are eligible to apply to this solicitation by reviewing the SVIP OTS 70RSAT21R00000006 section 4 and the eligibility section of the FAQ document posted with the topic call. Any applications received from ineligible applicants will be rejected.

5.3 General Instructions

5.3.1 Any invitations for oral pitches will be coordinated with the applicant and will be conducted via a virtual online meeting platform (e.g., MS Teams).

5.3.2 The Government may request applications for other Phases and will do so directly with the Company.

5.3.3 DHS S&T reserves the right to fund all, some, parts, or none of the applications received in response to this Topic Call.

5.4 Application Format, Instructions and Requirements

Applicants shall register in the OIP/SVIP Web Portal and complete all requested company information, upload the Technical and Cost Volume (TCV) as a PDF and submit the application prior to the final closing date and time. Applications are no longer being accepted by email.

Web Portal: The applicant shall register for an account, complete company information, apply to the Topic Call, upload the TCV and finalize their application submission.
Technical and Cost Volume (TCV): The TCV template can be found in the "Software Supply Chain Visibility Tools Topic Call and Analysis Application Guidance and Instructions" document posted with this Topic Call. The applicant shall provide technical and cost details associated with the proposed work. This shall be uploaded to the web portal when applying to the Topic Call.
Application: This is the final document that includes all of the information entered into the web portal and in the TCV once the submission process is complete. This will be the document reviewed by DHS.

After applicants have confirmed their eligibility, applicants **Shall** do the following:

Step 1: Register for an account through the OIP/SVIP Web Portal
Please see the "SVIP Portal Registration Guide" posted with this Topic Call. Please note you will need your company Tax Identification Number (TIN) for this step. If you don't have a TIN, instructions for receiving a temporary number are provided on the website**.**

Step 2: Apply to the Software Supply Chain Visibility Tools Topic Call through the OIP/SVIP Web Portal, proceed through each tab, answering all questions and complete the requested information.

- **Apply by the deadline of 10/3/22 12:00 PM PT/3:00 PM ET,** please select "SSCVT". Please note that the Portal will shut down right after the closing date and time even if you are still in the process of applying, so **DO NOT** wait until the last minute to submit.

Step 3: Under the Supporting Documents tab, complete the Software Supply Chain Visibility Tools Topic Call TCV (Template included in the "Software Supply Chain Visibility Tools Topic Call Application Guidance and Instructions" document posted with this Topic Call) and upload to the OIP/SVIP Web Portal.

- The TCV shall be in pdf format. Any other format will not be accepted.
- In addition to the REQUIRED TTA, at least one other TTA shall be selected in the TCV (see the check boxes in section 1.1 in the TCV template). If the proposed technology addresses multiple TTAs, check the applicable TTAs. Applicants shall not submit a separate TCV for each TTA; applicants shall address all applicable TTAs in one TCV.
  - All Sections of the application (both in the web portal and TCV) shall be completed. This includes sections with "Yes" and "No" boxes; applicants shall check one of the boxes.
  - The TCV including the Architectural/Intellectual Property diagram shall not exceed 8 pages.
  - The TCV shall describe the work proposed for Phase 1 and all questions shall be answered.
  - The Phase 1 amount shall not exceed $200,000.
  - Only content contained in the final application will be considered during the review process. No other documents, videos or links to information will be considered.

Step 4: Complete your application submission via the OIP/SVIP Web Portal

- Review and click the Submit button
- Applicants will receive a confirmation email once their application is successfully submitted.
- Applications shall be compliant with the aforementioned response dates and other compliance requirements in accordance with the DHS S&T SVIP 5-Year Innovation OTS (70RSAT21R00000006). **Submissions not in compliance shall be rejected.**

Applicants shall apply to the Topic Call using the portal as noted in the steps above. Please contact the portal helpdesk if you encounter any technical issues.

Monday - Friday

9:00 am - 5:00 pm ET
(571) 446-4869
OIPPortalHelpDesk@hq.dhs.gov

5.5 Evaluation Criteria

The OTS evaluation criteria published in the DHS S&T SVIP Other Transaction Solicitation 70RSAT21R00000006 will be utilized for the application evaluation process, and specific to this Call, applications will be reviewed for:

Criterion I: **Responsiveness to Technical Topic and Technical Approach**. The potential of the technology/solution to meet the project TTA goals provided in the OTS Call will be assessed, along with the technical and managerial approach to the proposed work.

- Applicability to the DHS illustrative use case(s) or other credible use case(s);
- Sufficient technical evidence that the solution will address the problem stated.

Criterion II: **Applicant's Capabilities and Related Experience**. The applicant's prior experience in similar efforts will be assessed to determine if the applicant clearly demonstrates an ability to deliver products that meet the proposed technical performance. The assessment for this criterion will include evaluating the experience of key personnel and any corporate viability requirements specified in a Topic call.

- Financial soundness of the company, and the business model based on the technology to be supported.

Criterion III: **Transition Approach**. A qualitative assessment will be made regarding how the proposed technology/solution will be transitioned to an operational user (e.g., commercialized or used by a DHS Component). The assessment will determine the likelihood that the applicant will be able to deploy a technology and/or solution(s) that can be transitioned effectively to the user community.

- The scalability and cost-effectiveness of the proposed technology or solution;
- Existing relationships with relevant end users, stakeholders and/or consumers;
- Ability to help DHS operational missions or critical infrastructure facilities.

5.6. Pitch Format and Requirements

Applicants invited to present pitches will be limited to fifteen (15) minutes for their pitch. In addition, applicants making pitches may provide up to ten (10) slides for presentation in either Microsoft PowerPoint or Adobe PDF. Embedded videos demonstrating current product capabilities are encouraged.

Create a user account and register their company in www.sam.gov

- This does not need to be done at the application phase but shall be done if the applicant is chosen to pitch and provides a successful pitch.

5.7 Contractual or Technical Inquiries

All contractual or technical inquiries to this OTS Call 70RSAT22R00000027 shall be emailed to DHS-Silicon-Valley@hq.dhs.gov. Emails submitting questions are to include **"Questions: Software Supply Chain Visibility Tools"** in the subject line. Questions will only be accepted and answered electronically.

5.8 Order of Precedence

In the event that any of the terms and conditions contained in this OTS Call 70RSAT22R00000027 conflict with terms and conditions included in SVIP 5 Year Innovation OTS (70RSAT21R00000006), the terms and conditions in this OTS Call 70RSAT22R00000027 shall take precedence.